WHAT IS CLAIMED IS:

1. An information processing apparatus comprising:

a) input means for inputting information data;

b) generation means for generating security data to be used to protect the information data;

c) encoding means for encoding the information data to generate encoded data;

d) extraction means for extracting a unique predetermined code indicating a specific meaning from encoded data within a security section in accordance with the security data;

e) superimposing means for superimposing the security data on the predetermined code;

f) scrambling means for scrambling the encoded data except for the predetermined code within the security section; and

g) output means for outputting the predetermined code processed by said superimposing means and the encoded data processed by said scrambling means.

2. An apparatus according to claim 1, wherein the security data contains key information to be used by said scrambling means.

3. An apparatus according to claim 1, wherein the security data contains information for an

authentication process.

4. An apparatus according to claim 1, wherein the information data is image data, and said encoding means generates an MPEG-4 bitstream.

5. An apparatus according to claim 4, further comprising IPMP encoding means for generating IPMP data indicating information that pertains to the security, and wherein said output means outputs the IPMP data generated by said IPMP encoding means.

6. An apparatus according to claim 1, further comprising enciphering means for enciphering the security data, and wherein said superimposing means superimposes the security data enciphered by said enciphering means.

7. An apparatus according to claim 1, wherein the predetermined code to be extracted by said extraction means is a start code.

8. An information processing apparatus comprising:

a) input means for inputting encoded data in which security data is adaptively superimposed on a unique predetermined code in the encoded data, which

indicates a specific meaning, and the encoded data except for the predetermined code is adaptively scrambled in accordance with the security data;

b) code extraction means for extracting from the encoded data a code which is located at a position where the predetermined code is present;

c) detection means for detecting the security data from the extracted code;

d) descrambling means for descrambling the encoded data in accordance with a detection result of said detection means; and

e) decoding means for decoding image encoded data descrambled by said descrambling means.

9. An apparatus according to claim 8, wherein the security data contains authentication data to be used to check authenticity, and said apparatus further comprises authentication means for checking authenticity.

10. An apparatus according to claim 8, wherein said descrambling means descrambles scrambled encoded data in accordance with a checking result of said authentication means.

11. An apparatus according to claim 1, wherein the security data is enciphered data, and said apparatus

further comprises deciphering means for deciphering the enciphered security data.

12. An apparatus according to claim 8, wherein the encoded data is MPEG-4 bitstream data.

13. An apparatus according to claim 12, wherein said input means inputs IPMP data indicating information which pertains to security.

14. An apparatus according to claim 13, wherein the IPMP data contains authentication data to be used to check authenticity, and said apparatus further comprises authentication means for checking authenticity in accordance with the authentication data.

15. An apparatus according to claim 14, wherein said descrambling means descrambles scrambled encoded data in accordance with a checking result of said authentication means.

16. An apparatus according to claim 15, wherein the security data is enciphered data, and said apparatus further comprises deciphering means for deciphering the enciphered security data.

17. An apparatus according to claim 8, wherein the predetermined code is a start code.

18. An information processing method comprising the steps of:

a) inputting information data;

b) generating security data to be used to protect the information data;

c) encoding the information data to generate encoded data;

d) extracting a unique predetermined code indicating a specific meaning from encoded data within a security section in accordance with the security data;

e) superimposing the security data on the predetermined code;

f) scrambling the encoded data except for the predetermined code within the security section; and

g) outputting the superimposed predetermined code and the scrambled encoded data.

19. A method according to claim 18, wherein the security data contains key information to be used in said scrambling step.

20. A method according to claim 18, wherein the security data contains information for an

authentication process.

21. A method according to claim 18, wherein said encoding step includes a step of generating an MPEG-4 bitstream.

22. A method according to claim 21, further comprising an IPMP encoding step of generating IPMP data indicating information that pertains to the security, and wherein said output step includes a step of outputting the IPMP data generated in the IPMP encoding step.

23. A method according to claim 18, further comprising an enciphering step of enciphering the security data, and wherein said superimposing step includes a step of superimposing the security data enciphered in said enciphering step.

24. A method according to claim 18, wherein the predetermined code to be extracted in said extraction step is a start code.

25. An information processing method comprising the steps of:

a) inputting encoded data in which security data is adaptively superimposed on a unique predetermined

code in the encoded data, which indicates a specific meaning, and the encoded data except for the predetermined code is adaptively scrambled in accordance with the security data;

b) extracting from the encoded data a code which is located at a position where the predetermined code is present;

c) detecting the security data from the extracted code;

d) descrambling the encoded data in accordance with the detection result; and

e) decoding the descrambled image encoded data.

26. A method according to claim 25, wherein the security data contains authentication data to be used to check authenticity, and said method further comprises an authentication step of checking authenticity.

27. A method according to claim 26, wherein said descrambling step includes a step of descrambling scrambled encoded data in accordance with a checking result in said authentication step.

28. A method according to claim 25, wherein the security data is enciphered data, and said method further comprises a deciphering step of deciphering the

enciphered security data.

29. A method according to claim 25, wherein the encoded data is MPEG-4 bitstream data.

30. A method according to claim 29, wherein said input step includes a step of inputting IPMP data indicating information which pertains to security.

31. A method according to claim 30, wherein the IPMP data contains authentication data to be used to check authenticity, and said method further comprises an authentication step of checking authenticity in accordance with the authentication data.

32. A method according to claim 31, wherein said descrambling step includes a step of descrambling scrambled encoded data in accordance with a checking result in said authentication step.

33. A method according to claim 31, wherein the security data is enciphered data, and said method further comprises a deciphering step of deciphering the enciphered security data.

34. A method according to claim 25, wherein the predetermined code is a start code.

35. An information processing method comprising the steps of:

a) inputting image encoded data that forms a hierarchical structure;

b) extracting a predetermined code indicating a head of a predetermined layer from the image encoded data; and

c) superimposing security data for image protection onto the predetermined code extracted in said extraction step.

36. A method according to claim 35, further comprising an enciphering step of enciphering the image encoded data in accordance with the security data.

37. An information processing method comprising the steps of:

a) inputting encoded data in which security data is superimposed on a predetermined code indicating a head of a predetermined layer of image encoded data that forms a hierarchical structure;

b) extracting from the encoded data a code which is located at a position where the predetermined code is present;

c) detecting the security data from the extracted code; and

d) decoding the encoded data in accordance with a

detection result.

38. A method according to claim 37, wherein the encoded data is enciphered data, and said decoding step includes a step of deciphering the enciphered encoded data.

39. A computer readable storage medium which stores a control program that implements an image processing method cited in claim 18.

40. A computer readable storage medium which stores a control program that implements an image processing method cited in claim 25.

41. A computer readable storage medium which stores a control program that implements an image processing method cited in claim 35.

42. A computer readable storage medium which stores a control program that implements an image processing method cited in claim 37.